AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1. (Currently Amended) An authentication method of at least one application working in an equipment connected by a network to a control server, said equipment being locally connected to a security module, said application being at least one of loadable and executable via an application execution environment of the equipment and ~~said~~ the at least one application being configured~~adapted~~ to use resources stored in the security module, the method comprising:

receiving by the control server, via the network, identification data including at least an identifier of the equipment and an identifier of the security module[[,]];

analyzing and verifying, by the control server, said identification data and, based on the analysis and verification, the control server creating a protection profile defining resources of the security module that can be used by the at least one application, the protection profile being created based on at least one of:

an updating of a version of a software installed in the equipment,

a downloading of a new application in the equipment,

an updating period of the protection profile,

a number of connection of the equipment to the network, and

a technology used for accessing the network[[,]];

generating, by the control server, a cryptogram, the cryptogram including a digest of the at least one application, the identification data, the protection profile ~~instructions intended for the security module~~ and at least one of an identifier of the at least one application and an identifier of security module resources[[,]]; and

transmitting the at least one application and the cryptogram by the control server, via the network and the equipment, to the security module, ~~and~~

wherein, when the at least one application and cryptogram are transmitted at a same time, the method includes,

verifying, by the security module, the at least one application by comparing the digest extracted from the received cryptogram with a digest determined by the security module, the verification occurring periodically at a rate given by the control server, during at least one of a first initialization of the at least one application, a first use of the at least one application, and each initialization of the at least one application, ~~wherein, during at least one of initialization and activation of the application,~~ the security module performs at least one of releasing and blocking access of certain resources of said security module to the at least one application based on the received protection profile, and

when the at least one application and the cryptogram are not transmitted at a same time, the method includes,

requesting by the at least one application, once loaded into the equipment from the control server via the network, the cryptogram from the server at the time of an initialization of the at least one application and transmitting the cryptogram to the security module, a confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the at least one application; and

performing the verifying by the security module when the cryptogram is accepted~~executes the instructions extracted from the cryptogram and, according to a result of the verification of the application, performs at least one of releasing and blocking access of certain resources of said security module to the application~~.

2. (Previously Presented) The method according to claim 1, wherein the equipment is a mobile equipment of mobile telephony.

3. (Previously Presented) The method according to claim 1, wherein the network is a mobile network of at least one of a GSM, GPRS, and UMTS.

4. (Previously Presented) The method according to claim 2, wherein the security module is a subscriber identification module that is inserted into the mobile equipment of mobile telephony.

5. (Previously Presented) The method according to claim 4, wherein the identification data of at least one of the mobile equipment and subscriber identification module includes an identifier of the mobile equipment and an identifier of the subscriber identification module pertaining to a subscriber of the network.

6. (Currently Amended) The method according to claim 1, wherein the protection profile~~instructions included in the cryptogram~~ received by the security module condition the use of the at least one application according to criteria established previously by at least one of the operator, the application supplier and the user of the equipment.

7. (Currently Amended) The method according to claim 6, wherein the criteria define limits of use of the at least one application according to risks associated with at least one of the software of the at least one application and the hardware of the equipment that the operator desires to take into account.

8-10. (Cancelled)

11. (Currently Amended) The method according to claim 1, wherein the cryptogram is generated with the aid of an asymmetrical or symmetrical encryption key from a data set including the identifier of the equipment, the identifier of the security module, an identifier of the at least one application, the digest of the at least one application calculated with an unidirectional hash function, identifiers of the resources of the security module and the protection profile~~instructions for blocking or releasing resources of the security module~~.

12. (Previously Presented) The method according to claim 11, wherein the cryptogram includes a variable that is predictable by the security module thereby avoiding the double use of a same cryptogram, the value of said variable controlled by the security module by comparing the value of the variable with a reference value, the reference value being stored in the security module and regularly updated.

13. (Cancelled)

14. (Currently Amended) The method according to the claim 1, wherein the cryptogram is transmitted to the security module at the same time as the at least one application is loaded into the equipment via the application execution environment.

15. (Cancelled)

16. (Previously Presented) The method according to claim 1, wherein the equipment is at least one of a Pay-TV decoder and a computer to which the security module is connected.

17. (Currently Amended) A system, comprising:

a~~A~~ security module including ~~comprising~~ resources that are~~intended to be~~ accessed locally by at least one application installed in an equipment, the equipment being connected by a network to a control server~~to a network,~~, wherein

the~~said~~ equipment includes~~including~~ means for reading and transmitting data, the transmitted data including at least one of an identifier of the equipment and an identifier of the security module, and

the~~said~~ security module includes,

~~further including~~ means for reception, storage and analysis of a cryptogram and of the at least one application received with the cryptogram, the cryptogram and the at least one application being transmitted by the control server,

wherein the control server analyzes and verifies the transmitted at least one of the identifier of the equipment and the identifier of the security module, and the control server creates a protection profile defining resources of the security module that can be used by the at least one application, the protection profile being created based on at least one of:

an updating of a version of a software installed in the equipment,

a downloading of a new application in the equipment,

an updating period of the protection profile,

a number of connection of the equipment to the network, and

a technology used for accessing the network, and

wherein ~~wherein~~ the cryptogram includes a digest of ~~said~~ the at least one application, at least one of the identifier of the equipment and the identifier of the security module, the protection profile~~instructions for the security module~~, means for verifying said at least one application, and means for identification of security module resources, and

means for extraction and execution ~~of the instructions contained in the cryptogram~~, wherein

when the at least one application and cryptogram are received at a same time, the means for extraction and execution perform ~~performing~~ at least one of releasing and blocking certain resources of the security module to the at least one application according to the received protection profile, and verifying ~~a result of the verification of~~ the at least one application, the verification occurring periodically at a rate given by the control server, during at least one of a first initialization of the at least one application, a first use of the at least one application, and each initialization of the at least one application, and

when the at least one application and the cryptogram are not received at a same time,

the at least one application, once loaded into the equipment from the control server via the network, requests the cryptogram from the server at the time of its initialization and transmits the cryptogram to the security module, the confirmation message of acceptance or refusal of the cryptogram being transmitted by the security module to the server via the at least one application, and

the means for extraction and execution perform at least one of releasing and blocking certain resources of the security module to the at least one application according to the received protection profile, and verifying the at least one application, the verification occurring periodically at a rate given by the control

server, during at least one of a first initialization of the at least one application, a first use of the at least one application, and each initialization of the at least one application.

18. (Currently Amended) The systemsecurity module according to claim 17, wherein the security module is a subscriber identification module that is connected to a mobile equipment.

19. (Previously Presented) The method according to claim 2, wherein the security module is a subscriber identification module that is inserted into the mobile equipment of mobile telephony.

20. (Cancelled)

*** END CLAIM LISTING ***